I
N
S
I
D
E

Reliability of Fault-Tolerant Computing Systems and Networks

*By: Martin L. Shooman, Polytechnic University, Brooklyn, NY
and Martin L. Shooman & Associates*

Introduction

The complexity of modern digital systems, made more problematic by the microelectronics revolution, is a "two-edged sword." Complexity creates both the need for fault tolerance and the means to implement various solutions. With fault-tolerant computing, correct output is obtained in spite of the presence of internal errors called faults. Any system with redundant components or functions can be made fault-tolerant. For the designer who keeps fault-tolerance in mind during the early stages of design, many techniques are available: error-correcting codes added to input, internal, and output data streams; parallel, standby, or voting redundancy schemes; and where applicable, parallel paths through a network. Software also can be made redundant if one employs two independent software teams to develop different yet functionally identical versions of the software; however, any common errors will limit the redundant effect.

Availability. Redundancy also provides an opportunity to significantly increase the reliability, the probability of no system failure, by introducing the possibility of repair during system operation. Furthermore, the availability, the probability that the system is up, is often computed from the ratio of (uptime)/(uptime + downtime), which also measures the beneficial effects of repair. The analysis of system availability generally involves the formulation and solution of a Markov probability model. The use of Laplace transforms and appropriate use of simplifying theorems greatly facilitates the analysis effort and provides insight into system behavior. The design of a large system often is driven by functional requirements; however, when reliability considerations are included, the apportionment of redundancy throughout the system can be used as a means of optimizing redundancy. There are several simple, heuristic apportionment schemes as well as a new technique of reliability optimization, which uses upper and lower bounds to limit the computations to a modest number of feasible solutions.

Typical System Reliability and Availability. The reader can appreciate some of the gains in system reliability and availability achieved in the last half of the 20th century by studying the comparison in Table 1.

Coding

Everyone knows the cliché describing computer systems – "Garbage in, garbage out." One might describe error-correcting codes as "Garbage in, correct information out." This is accomplished by adding extra (redundant) bits to the input that act as error checks. Schemes such as adding redundant bits are used to detect and correct errors in bit "transmissions" that occur in communication (e.g., modems, satellites, etc.), memory reads and writes in a CPU, and computer network messages.

One can assume that errors in transmitted binary words occur due to noise that affects individual bits in a word, causing errors, i.e., zero bits corrupted to ones or one bits corrupted to zeroes. Assume that noise is rare and occurs in short pulses with duration less than the width of a transmission pulse. The simplest technique for error checking is to transmit each word twice, and then sequentially compare each bit in the first transmitted word with the corresponding bit in the second transmitted word. If a given bit is the same in both words, the bit is passed. If not, an error is detected and word can be retransmitted until two identical copies are then obtained, correcting the error. Clearly, this scheme at least

Table 1. Comparison of Reliability and Availability for Various Fault-Tolerant Systems (Reference 3, pages 16, 17)

Application	Reliability	Availability*
1964 NASA *Saturn Launch* computer	R(250 hr.) = 0.99	------
Apollo NASA Moon Mission	R(mission) = 15/16 = 0.938	------
NASA Space Shuttle	R(mission) = 109/110 = 0.991 Through flight 110 in April 2002. Note: Challenger flight exploded on 1/28/86.	------
Bell Labs' ESS Telephone Switching System, 1966	------	Requirement of 2 hr. of downtime in 40 yr. 0.9999943
Tandem computer goals in 1980s	------	Tandem goals 0.999996
Stratus computer (web site quote 2001)	------	Stratus quote 0.9999905
Vintage 1985 Single CPU, transaction-processing	------	0.997 [Reference 4, p. 586]
Vintage 1985 Two in parallel CPU, transaction-processing	------	0.999982
Vintage 1985 Two in standby CPU, transaction-processing	------	0.9999911

*Note that the ESS availability goal of 40 years is clearly a steady state availability. Although not stated, the Tandem, Stratus, and Vintage 1985 numbers as well as the derived parallel and standby system availabilities are undoubtedly steady state values.

doubles the length of each transmitted word (i.e., 100% or more overhead is required for error detection). More efficient methods exist with less overhead.

Parity Bit Codes. The simplest scheme is to append a single bit called a *parity* bit to the word. If an even or odd parity scheme is chosen, the parity bit is set to 1 or 0 so that the number of 1s in the word (including the parity bit) is an even or odd number respectively. The parity bit is generally computed using a "tree" network of EXOR gates. The information word with parity bit attached is then transmitted and when the word is received, another EXOR tree is used to check that the parity is still even or odd. Clearly this scheme detects single, triple, and any odd number of bit errors. If the scheme is applied to an 8-bit byte, the parity bit is a ninth bit and the overhead due to checking is 12.5%. Parity bit error detection codes have such small overhead that they are used in a wide variety of applications. There are inexpensive, standard code generation (coder) and checking (decoder) digital circuits (74LS280).

Of course the code does not detect double, quadruple, or any even number of errors since the parity is not changed in these cases. The probability of an undetected error is the probability that an even number of errors occur, which can be approximated by the most significant term – the Binomial probability of two errors out of nine bits, which is given by $36q^2 (1 - q)^7$ where q is the probability of bit error. Without parity bit checking, all errors are undetected and the binomial probability of one or more errors in 8 bits is given by $1 - (1 - q)^8$. The ratio of these two expressions gives the error reduction factor due to parity codes that can be as large as 2×10^7 when $q = 10^{-8}$. This analysis neglects the possibility that an undetected error can occur due to a failure of the coding or decoding circuitry. When these failure probabilities are included in the analysis, the error reduction factor is decreased, especially for low transmission rates and small values of q. For such values one has to wait many days or years

before multiple errors occur and the probability of chip failure during this time period becomes significant. The results for a parity bit code are shown in Figure 1, where the downward curve at the top left of the diagram is due to chip failures.

Hamming Codes. The parity bit code is the least complex of the many code types commonly used and is the simplest member of an entire family of codes developed by Hamming [Reference 1] that use extra check bits to detect multiple errors and correct some errors. Although the more complex Hamming codes have higher overhead, their error-correcting ability accounts for their wide usage. Thus, Hamming Single Error Correcting and Single Error Detecting (SECSED) and Hamming Single Error Correcting and Double Error Detecting (SECDED) codes are popular. All Hamming codes assume that the probability of multiple errors in a transmitted word is small; however in the case of many storage devices, such as CDs, CD-ROMs, DVDs, hard and floppy disk drives, errors often occur in bunches called bursts. Bursts require a different formulation and the Reed-Solomon (RS) code is commonly employed, [Reference 5].

Redundancy

Four major approaches are used to improve system reliability: (1) simplify the system to use fewer components or simpler algorithms and software; (2) lower component and software failure rates; (3) provide redundant components or logical paths through the system; and (4), for redundant components, repair failed hardware and software components restoring full redundancy. In this section, we will assume that the system designer has taken advantage of (1) and (2) although this is not always the case in practice, and focus on (3) and (4). One can view the material covered in the last section of this article on apportionment and redundancy optimization as an extension of redundancy as described in this section.
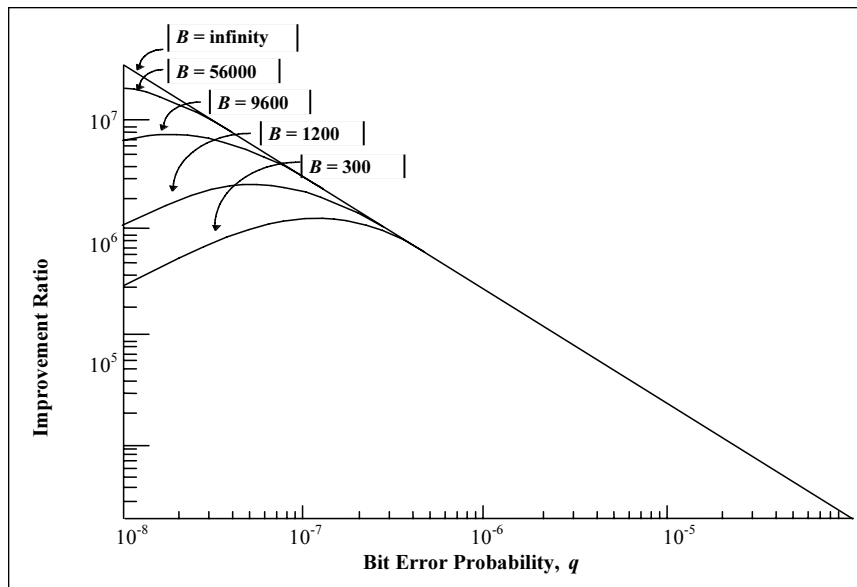
*Figure 1. Undetected Error Improvement Ratio for a Single Byte with a Parity Bit Versus Error Probability q and Transmission Rate B in Bits per Second (*Reference 3, *Figure 2.5, page 45)*

In general redundancy improves system reliability (and availability) because it provides alternate paths through the system so that if one fails, there is another that continues operation. Redundancy was prevalent during the era of analog circuitry in the mid 20th century. However, with the advent of digital circuitry in the later half of last century, it became easy to implement a wide variety of simple as well as complex redundancy schemes.

System and Component Redundancy. Most systems are composed of components. Thus, reliability can be considered at a system or component level. Consider, for example, a system composed of two components A and B that must both work for successful operation. If one employs *system* redundancy, a second system A'B' is connected in parallel so that if either system fails, the second system takes over. If components A and B have an equal probability of failure q, then a *single* system has an approximate probability of failure of 2q. In the case of *system* redundancy, both AB and A'B' must fail for the system to fail and if the two replicas are identical the approximate probability of failure is (2q) x (2q) = $4q^2$.

However, there is another possibility of using *component* redundancy, i.e., to parallel A and A' and parallel B and B'. In such a case, the failure probability of the AA' cluster is approximately q^2 and that of the BB' cluster is approximately q^2 and the failure of either cluster $2q^2$. Thus, the reliability using system redundancy is superior to a single system ($2q > 4q^2$), and the reliability using component redundancy is still better ($2q > 4q^2 > 2q^2$). Detailed analysis verifies this result.

Thus far, we have neglected the device needed to connect items in parallel, which can be termed the coupling device. A complete analysis of the two redundancy schemes just discussed requires including the reliability of the coupling device. Clearly, the relia-

bility of the coupling device appears as a series element and when system reliability is used one coupling device is required and the reliability of the coupler is r_c. If there are five major components in the system and component redundancy is used, the reliability of the system of couplers is $(r_c)^5$. If coupler unreliability is significant, it can erode the advantages of component reliability over system reliability, and a detailed analysis is needed.

Standby Systems. In a parallel system the extra redundant system(s) or component(s) is powered up and can fail although only one system or component is needed for system operation. A standby system improves on this situation by using one on-line system or component to provide operation and keeping the power off for the standby elements. As long as the non-powered standby elements have very low or zero failure rates, the standby system is superior to the parallel system. The reliability of a single element with a constant failure rate λ is $r_s = e^{-\lambda t}$ and that of a parallel system is $r_p = 2e^{-\lambda t} - e^{-2\lambda t}$. One can show that the reliability of a standby system is $r_s = e^{-\lambda t} + \lambda t e^{-\lambda t}$ and that it is always better than a parallel system.

However, the reliability of the coupler can have a significant effect on the results. In the case of a standby system, the "coupler" is more complex than in a parallel system. In essence it is a smart switch, which detects the failure of the on-line unit, powers up the standby unit, and switches the inputs and outputs to the standby unit. A simple comparison of the two systems can be made by neglecting the coupler effect in a parallel system and assuming that the reliability of the switch in a standby system is given by $e^{-\lambda_s t}$ and that it multiplies the expression for r_s. A comparison of the two expressions is given in Figure 2. This analysis shows that the standby system is superior to the parallel system as long as the failure rate of the switch is 0.5λ or smaller.
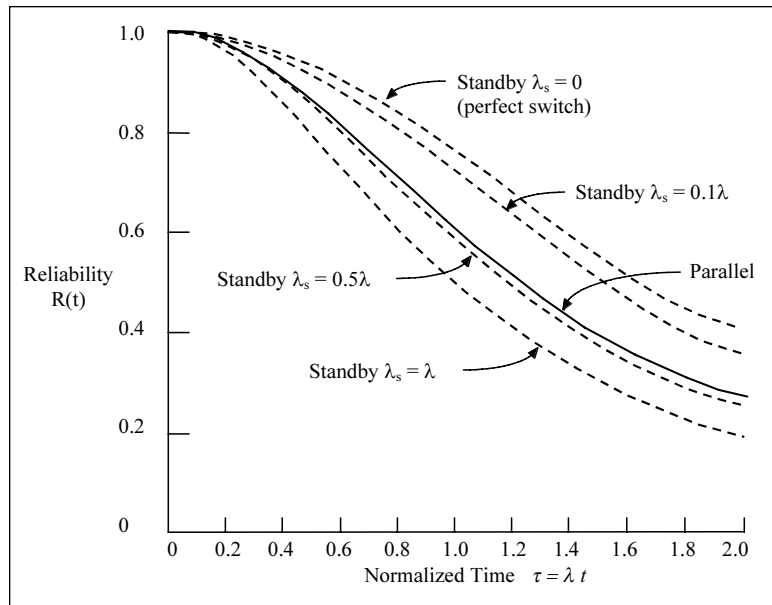
Figure 2. A Comparison of a Two-Element Ordinary Parallel System with a Two-Element Standby System with Imperfect Switch Reliability (Reference 3, Figure 3.13, page 110)

Repair. Repair can further improve reliability in a system with redundancy when repairs of failed redundant paths can be made while the system continues to operate. The beneficial effects of repair in the case of a parallel or standby system are obvious. When one item fails, it is repaired while the other item continues operation. The system only fails if the remaining unit goes down before the failed unit is repaired and placed back in service.

Thus, it is a race to see whether repair occurs before a second failure happens. However, the repair rate is much larger than the failure rate in all practical cases; thus, repair continues to win for many cycles and the time to system failure is greatly increased by repair. For example, in the case of an automobile, we might estimate that the failure rate (unscheduled maintenance) is once per year. However, the repair plus waiting time is typically about one day yielding a repair rate of 365 repairs per year.

Markov Models. For a complete analysis of repair effects, we must make a Markov model for the system with repair. The first step is to identify the system states. As an example let us consider two elements with repair (either parallel or standby). The elements are one and two and the state where both are good is S_0 = $x_1 x_2$ where both are bad S_2 = $\bar{x}_1 \bar{x}_2$ and where one is good S_1 = $x_1 x_2$ + $x_1 \bar{x}_2$. These three states are shown as nodes in Figure 3. The arcs between states, which go from left to right, represent failures and are labeled with failure rates λ and the arcs directed from right to left represent repair and are labeled with repair rates μ. The probability of being in each of the states is obtained by solving a first order differential equation for each probability and, since the equations are coupled, the solution becomes that of a third order differential equation. The Laplace transform method can be used to simplify the solution work, however much algebra is still involved. However, if we are satisfied with

less than the complete solution three Laplace transform theorems for the initial value, the final value, and the integral of a function can be used to easily find: (a) the mean time to failure, (b) the final value, and (c) the Taylor series approximation for the initial behavior. If we are only interested in the system mean time between failure, MTBF, we obtain the results given in Table 2. Note that if the repair rate is 10 times the failure rate, a standby system has 12 times the MTTF of a single element, which is 6 times better than without repair. For practical systems where the repair rate greatly exceeds the failure rate, very large gains in system MTTF are realized.
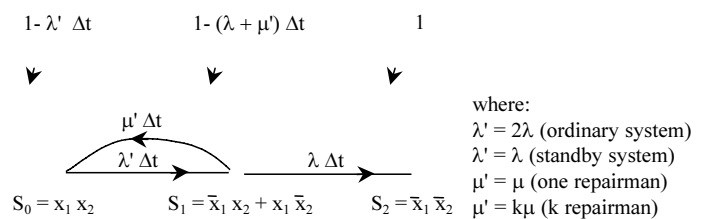

Figure 3. A Markov Reliability Model for Two Identical Parallel Elements and k Repairmen (Reference 3, Figure 3.14, page 112)

Table 2. Comparison of the MTTF for the Various Systems Represented by Figure 3 (Reference 3, page 115)

Element	Formula	MTBF For $\lambda = 1$, $\mu = 10$
Single	$1/\lambda$	1.0
2 parallel – no repair	$1.5/\lambda$	1.5
2 standby – no repair	$2/\lambda$	2.0
2 parallel – repair	$(3\lambda + \mu)/2\lambda^2$	6.5
2 standby – repair	$(2\lambda + \mu)/\lambda^2$	12.0

Related Concepts. Space does not allow a full description of many related issues; however, a few will be briefly discussed.

Availability: Reliability measures the probability that a system is always up, working in interval 0 to t. However, cases when a system goes down for a few minutes and is quickly repaired are considered examples of good availability. Availability is the probability of being up at time t (even if it has failed and been repaired one or more times) and can be calculated from a Markov model such as the one shown in Figure 3, if an additional repair branch is added from state two (S_2) back to state one (S_1).

Coverage: In a standby system the "coupler" must sense failure of the on-line element and switch in the standby one; otherwise the system fails. Since the coupler cannot detect all failures, one should model the fraction detected (called coverage) in a Markov analysis. Typical values for coverage are 0.90 and 0.95. Low coverage can significantly decrease the improvement in reliability achieved with redundancy.

N-Modular Redundancy: The problems in designing a reliable coupling device in a parallel or standby system can be avoided if N-Modular redundancy is used. In the most common case, N = 3, and the method is called TMR, triple modular redundancy, where three copies of a digital circuit are employed and their outputs are compared in a simple digital circuit that produces an output agreeing with the majority. Thus, the system succeeds if there are no failures or one failure, the reliability is better than a single component in the high reliability region, (λt is small), and the availability can be high with repair.

NonStop Computing: Many computing applications require very high levels of reliability and availability and Tandem computers (now a division of Compaq) coined the term NonStop computing in the 1980s to appeal to the on-line transaction processing market. Their system utilized software and hardware redundancy, as did their competitor Stratus, to achieve high levels of availability, (see Table 1).

RAID: Data storage in modern computer system is generally implemented using a Redundant Array of Independent Disks (RAID). Many RAID techniques employ redundant disks and error-correcting bits applied to the data and spread over many disks. These techniques utilize 50 to several hundred disks and achieve huge storage densities and high reliability.

Networks

Much of the world is interconnected by a network(s). For many, this is the Internet at home and a local area network at work linking computers, printers, workstations, and the Internet. Several methods can be used to compute the reliability and availability of a network. However, we will focus on the most straightforward approach. First, one should state that the network field uniformly computes the availability of a network and call this the

"network reliability." The model of a network is based on the mathematical graph of the network where network nodes (vertices) represent computers, printers, terminals, etc. and the branches (arcs) in the network represent the communication links between the nodes. The simplest model assumes that the nodes do not fail but the links do. We define a path as a collection of branches that provides communications between a specified pair of nodes.

The four-node network shown in Figure 4 has six branches. One method of analyzing the network is to examine all combinations of the six branches, where each branch can be either up or down. For example, the combination called event 41 is denoted by E_{41} = 1'23'4'56 where links 1, 3, and 4 are down but 2, 5, and 6 are up. The combination E_{41} provides a path between nodes a and b, so we would say that E_{41} provides two terminal connections between ab. A detailed study of E_{41} shows that it also provides a connection between all the other node pairs. Thus, we can say that E_{41} provides all terminal connection. Since each of the branches has two states (up and down) and there are 6 branches, there are $2^6 = 64$ different combinations of events. All of the events as formulated are mutually exclusive. Thus, the two terminal reliability between nodes s and t is the sum of the probabilities of each event that provides connection between s and t. Similarly, the all-terminal reliability is the sum of the probabilities of all the events that provide all terminal connection. Again, we emphasize that the term reliability really means availability because we speak of each branch being up or down, which means that they can fail and be repaired.
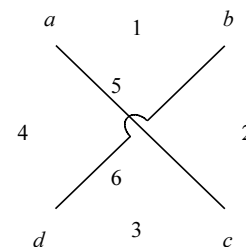

*Figure 4. A Four-Node Graph Representing a Computer or Communication Network (*Reference 3*, Figure 6.1, page 285)*

The preceding method for calculating reliability is called "State-Space Enumeration" and will become clearer as we fill in the details for calculating the two terminal reliability, R_{ab}. The easiest way to explore the 64 combinations is to group them by the number of failed branches and explore each grouping. There is only one combination of no failures, E_1 = 123456, and clearly this provides a connection between a and b. There are 6 combinations of one failure and all provide connection between a and b: E_2 = 1'23456, E_3 = 12'3456, E_4 = 123'456, E_5 = 1234'56, E_6 = 12345'6, and E_7 = 123456'. Clearly, as long as edge 1 is up, there is a connection, and E_3 through E_7 provide a connection. In the case of E_2 although 1 is down, 25 provides a connection. In a similar manner, all the events are explored and the conclusion is that there are 48 good events, [the details are given in

Reference 3, pp. 288-292]. The reliability expression is given by Equation (1).

$$R_{ab} = [P(E_1)] + [P(E_2) + \cdots + P(E_7)] + [P(E_8) \quad (1)$$
$$+ \cdots + P(E_{22})] + [P(E_{23}) + \cdots + P(E_{34})$$
$$+ P(E_{37}) + \cdots + P(E_{42})] + [P(E_{43})$$
$$+ \cdots + P(E_{47}) + P(E_{50}) + P(E_{56})] + [P(E_{58})]$$

If all edges are identical and have a probability of being up of p and a probability of being down of q, then Equation 1 becomes:

$$R_{ab} = p^6 + 6\,p^5q + 15\,p^4q^2 + 18\,p^3q^3 + 7\,p^2q^4 + pq^5 \quad (2)$$

For the case where p = 0.9 and q = 0.1, substitution in Equation (2) yields an availability of 0.997848. To improve network reliability we would have to increase p or add more branches to the network.

Many other more sophisticated techniques are available for computing the availability of a network, including approximate techniques and computer programs to help with the computations. There are network design techniques that help with the design of a reliable network given a set of nodes to connect, and others that suggest how to obtain the biggest increase in reliability by adding additional branches to an existing network.

Apportionment and Redundancy Optimization

In discussing redundancy in the preceding section, it was assumed that the unit in question was a component or a modestly sized system. A more global issue is, given a large system that has unsatisfactory reliability or availability, how can we best improve the reliability or availability by using a limited amount of redundancy in the system. This is essentially top down redundancy and although less efficient than bottom up redundancy, it fits in well with a system engineering approach to system design.

Assume a block diagram represents the overall structure of the system, where each level of decomposition is represented by n submembers. If the decomposition produces 2 or 3 submembers, too little decomposition occurs; if there are more than 10 submembers things are too complex. For a rationale for why 5-9 submembers is a good goal [Reference 3, pp. 337-342]. In general, one has an overall system goal R_s (or A_s) and the reliability of all the submembers combine to yield the system reliability. If all the n submembers are independent and have an equal reliability r, then $R_s = r^n$. Since we know R_s we can solve for r obtaining r = $(R_s)^{1/n}$. This is a gross approximation and an easy first start. Assigning a set of reliabilities for the submembers that equals the system goal is generally called apportionment.

A brief study of the reliability of each of the submembers will show how easy it is to reach the r goal for each submember. In general, some are reachable and some will be very difficult. Seldom does one discover that all the submember goals are easily met. However, sometimes all of them appear to be insurmountable goals. A better procedure than the equal reliability assumption is to use the preliminary analysis of the subsystems to establish a set of ratios of the initial failure rates. Suppose that n = 5 and the initial design of subsystems one and two seem to have roughly equal reliabilities and a failure rate λ, then $\lambda_1 = \lambda_2 = \lambda$. However, suppose three and four are more difficult and have roughly double the failure rate, $\lambda_3 = \lambda_4 = 2\lambda$. Furthermore, subsystem 5 is the most difficult and has a failure rate $\lambda_5 = 6\lambda$. Although these are all just initial estimates, one can use them to obtain a better second round of estimates. The system reliability becomes:

$$R_s = (e^{-\lambda t})(e^{-\lambda t})(e^{-2\lambda t})(e^{-2\lambda t})(e^{-6\lambda t}) = e^{-12\lambda t} \quad (3)$$

Solving for λ yields $\lambda = -\ln(R_s)/12$ and, using this value for λ, we obtain reliability goals for each of the submembers. It is always useful to apply these simple techniques of apportionment (and sometimes the more complex procedures [Reference 3, pp. 342-351]) in the initial design stages.

One can formulate a more exact approach to reliability optimization using redundancy. As an example, assume that n = 3, that the initial estimates for the reliability of each subsystem is $R_1 = 0.85$, $R_2 = 0.5$, and $R_3 = 0.3$. The system goal is $R_g = 0.9$; however, the initial design has a reliability of 0.85 x 0.5 x 0.3 = 0.1275. Each subsystem has a cost of 1 unit and the total cost budget is 16 units; thus 13 units are available to assign parallel elements to the three subsystems to achieve the system reliability goal. Our objective is to find the set of solutions where the system reliability $R_s \geq R_g$, the cost of each of these solutions, and then to choose among these possibilities.

A brute force approach is to recognize that given the cost constraints, we could assign to subsystem one, 0 to 13 parallel redundant units. Similarly, there are 14 different choices for subsystems two and three, and the total space of possible combinations is 14 x 14 x 14 = 2,744! Clearly with modern computational power, a brute force computation and ordering of the 2,744 cases is possible. However, such an approach becomes impossible for any practical size system. In the past, gradient search approaches (greedy algorithms) and dynamic programming have been used to reduce the number of cases that must be compared [Reference 3, pp. 369-378]. Recently, a bounded enumeration approach has been discovered that allows a great reduction in effort – only 10 combinations need to be explored [Reference 3, pp. 351-366]. The first bounds to apply are the lower bounds that are derived from the fact that each subsystem must have a reliability equal to or exceeding the system goal and these bounds assume all other subsystems have a reliability equal to unity. Thus,

$$(1 - [1 - R_i]^{n_i}) \geq R_g \quad (4)$$

Solving for n_i from Equation (4) yields:

$$n_i = \log(1 - R_g)/\log(1 - R_i) \quad (5)$$

For the three subsystems of our example, $n_1 = 1.21$, $n_2 = 3.32$, and $n_3 = 6.46$. Rounding to the next highest integer, $n_1 = 2$, $n_2 = 4$,

Industry News

Veterans Administration to Reimburse for CPL Exam Fees

by: Robert H. Pratt, SOLE HQ Volunteer

Effective with the May 2001 Exam (Exam 55), anyone who is eligible for the Montgomery GI Bill; or Veterans Educational Assistance Program (VEAP)/Dependents Educational Assistance Program (DEAP) benefits can have his/her Certified Professional Logistician (CPL) program examination fees (both initial and retake) reimbursed by the Department of Veterans Affairs (VA).

The reimbursement arrangement was a result of a recent change in Federal law related to tests for professional certification and licensure. SOLE's CPL certification program was the first in Maryland to be approved for coverage under the new law. The approval, granted in July 2001 by the Maryland Higher Education Commission as agent for the VA (and made retroactive to the May 2001 exam), applies to all eligible veterans/dependents, regardless of state of residence.

The approved categories and fees are:

- Certified Professional Logistician Examination, non-SOLE member – $275.00
- Certified Professional Logistician Examination, SOLE member – $125.00
- CPL Retake Exam – $50.00

(Qualified individuals should note that the VA can pay only for the cost of the test, and not other fees connected with obtaining the certification.)

Individuals who qualify for the benefits must first take the exam, then apply to the VA for reimbursement. To be reimbursed, the individual should send a copy of his/her test results to the VA office that handles his/her benefits. The VA's Internet site – <www.gibill.va.gov/education/inquiry.htm> – should be checked **before** the exam is taken.

Those who have never applied for VA benefits will also need to submit either VA Form 22-1990 (to be completed by veterans or those on active duty); or VA Form 5490 (to be completed by the eligible child or spouse). These forms may be filled out on-line at <www.va.gov>. Alternatively, the forms may be requested by calling the VA's toll-free telephone number, (888) 442-4551. (The VA's toll-free telephone number for the hearing impaired is (800) 829- 4833.)

Honeywell Troubleshoots Engines on the Internet

It seems that with each day that passes, new and creative web sites appear. One of the most useful is a web site developed by Honeywell in collaboration with Casebank Technologies. At the site, <https://www.e-engine.Honeywell.com>, Honeywell provides personalized maintenance and operations support to business, general aviation, and regional airline customers operating TFE731, TPE331, and other engines. Services provided include:

- Trending (Engine Condition Trend Monitoring [ECTM] and Jet-Care Analysis)
- Training
- Diagnostics
- Technical publications
- Electronic logbooks (compatible with Aircraft Technical Publishers maintenance director software)
- Upgrades/Retrofits
- SOAP Analysis
- Communications tools for operators and service centers

The web site has been operating since the end of 2000. Spotlight, a troubleshooting tool, was added in June of this year. Honeywell plans to incorporate additional troubleshooting tools for auxiliary power units and the CF738 and AS907 engines by early 2003. From September 2001 to August 2002, more than 40,000 logons to the web site were recorded.

Detecting Fatigue Failures Using Positrons

A new technology for the non-destructive inspection (NDI) of materials has been demonstrated by Positron Systems, Inc. The new technology, Photon Induced Positron Annihilation (PIPA), can detect fatigue failures in second layer materials. The demonstration was conducted at Positron's Systems' Test and Analysis Center on wing spar samples provided by Sandia Laboratories.

According to Positron, the new technology is "A fundamental advancement in nondestructive testing that identifies structural integrity, fatigue, and embrittlement problems at the atomic level." Traditional NDI methods, such as eddy current and x-ray, are useful only after a visible crack or deformity has progressed to the crack initiation phase. PIPA can detect fatigue, embrittlement, and material lattice damage at an atomic level, prior to the crack initiation phase.

PIPA works by generating positrons inside a bulk material or component being examined, followed by annihilation of those positrons with electrons in the material (see Figure 1). The gamma spectrometry response of the positron annihilation is then measured and is highly quantitative and accurate.

Positron annihilations produce 511 KeV gamma rays; however, the total energy released includes the momentum energy of the electron with which the positron annihilates. Positron annihilations in defective material occur with low-momentum free electrons. Consequently, the gamma-ray energy produced is at or near the 511 KeV.
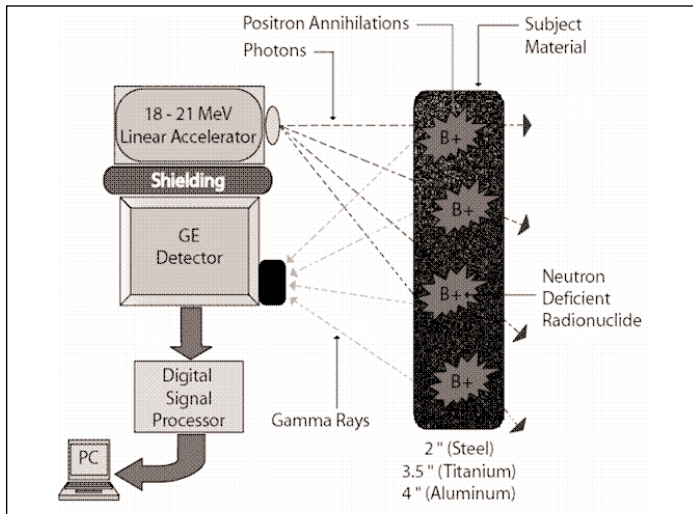
Figure 1. The PIPA Process

From these gamma spectrometry response data and Positron Systems' analytical methods, quantifiable fatigue or embrittlement damage estimates are produced. Data can be obtained not only on the concentration of defects, but also the type and size of defects by using the coincidence lifetime method.

PIPA is intended to be used to:

- Detect fatigue, embrittlement, and defects at the atomic level
- Find damage before cracks appear
- Work on a variety of materials
- Predict remaining life of expensive components

Positron believes that PIPA will be a key element of any structural integrity program and be useful in a wide range of applications, from aircraft landing struts and wing spars to nuclear power plants and oil refineries. For more information, visit Positron's web site at: <http://www.positronsystems.com/>.

SEI Announces Transition to CMMI

The purpose of this announcement is to establish January 1, 2003 as the date by which all users of the CMMI Product Suite are expected to have made the transition from previous versions of the CMMI Product Suite to Version 1.1 for process improvement and process appraisals.

This means that you should be using Version 1.1 of each of the following by January 1, 2003: CMMI models, SCAMPI[SM] Method Definition Document, and Introduction to CMMI training materials.

Making this transition to Version 1.1 will help ensure:

- A common standard of reference is being used throughout the community for appraisals and process improvement.

- The community benefits from the clarifications and improvements made in the Version 1.1 products.
- Appraisal results (i.e., the Maturity Profile) are reported in a way that improves the meaning and comparability of the results.

As of January 1, 2003, CMMI appraisals that do not use SCAMPI Version 1.1 and a Version 1.1 CMMI model will not be accepted by the SEI (unless they report on an appraisal that occurred before January 1, 2003).

SCAMPI Lead Appraisers [SM], CMMI course instructors, EPG and SEPG members, and others who have already attended CMMI model training (i.e., Introduction to CMMI or CMMI Intermediate Concepts) do not need to attend Version 1.1 training; however, they are responsible for gaining knowledge of the newest version of the models. Complete Version 1.1 models and model comparison files to aid this activity are available on the CMMI web site:

- CMMI Models
  <http://www.sei.cmu.edu/cmmi/models/models.html>
- Comparison of Version 1.1 and Version 1.02 CMMI Models
  <http://www.sei.cmu.edu/cmmi/models/compare.html>
- Comparison of CMMI-SE/SW/IPPD/SS Version 1.1 to Related Models
  <http://www.sei.cmu.edu/cmmi/models/sscompare.html>

RMQS Headlines

[Editor's Note: In this issue, we introduce a new feature; RMQS Headlines. The idea is to provide the headlines and short abstracts of articles on reliability, maintainability, quality, and supportability appearing in other publications and newspapers. Please E-mail me at <ncriscimagna@iitri.org> and let me know if you like the feature.]

Navy-Air Force Plan to Modernize Electronic Warfare is "Unconvincing," National Defense Magazine, published by NDIA, October 2002, page 12. The only electronic jammer in the military, the twin-engined EA-6B Prowler is getting old and less reliable. Maintenance and spares problems are increasing for the aircraft, the first of which rolled off the assembly line in 1969.

Ship Maintenance Still Far From the Information Age, National Defense Magazine, published by NDIA, October 2002, page 23. Corrosion is a maintenance nightmare, and applying non-skid surfaces to the flight deck is costing millions of dollars. Automation technologies have not helped these or other shipboard maintenance and servicing problems.

First, Do No Harm: Is there a nondestructive testing method that's right for you? Quality Digest, published by QCI International, October 2002, page 33. The value of nondestructive test is explored and a variety of methods are described.

Unreliable System Costs >75,000 Patients Lives Annually, Reliability Review, published by the Reliability Division of ASQ, September 2002, page 3. Poor process reliability is resulting in the spread of infections in hospitals leading to more than 75,000 deaths annually. These infections are preventable if the same approach used to develop and control industrial processes is applied by hospitals.

Step-Stress Accelerated Life Testing: Test Plan, Model, and Application, Reliability Review, published by the Reliability Division of ASQ, September 2002, page 13. A plan and model for conducting accelerated life testing is presented together with a case study in which the model is applied.

Human Systems Integration, Program Manager, published for the Defense Acquisition University, July-August 2002, page 88. The authors explore the importance of designing for interaction of human beings with everything in the environment associated with systems. They describe the organizational and analytical processes associated with human systems integration.

ISO/TS 16949 the Clear Choice for Automotive Suppliers, *Quality Progress*, published by ASQ, October 2002, page 44. General Motors Corp., Daimler-Chrysler, and Ford Motor Company are requiring their suppliers to transition from QS-9000 to ISO/TS 16949 and to be certified for the latter by July 2004. The change is intended to facilitate access to various world markets.

Reliability of Fault-Tolerant . . . (Continued from page 6)

and $n_3 = 7$. Thus, 13 units have been allocated (including the initial 3), and only 3 cost units are left. Consequently, four additional possibilities remain for each of the three units, 0,1,2,3 additional units, and the number of cases to enumerate is 4 x 4 x 4 = 64. This number can be further reduced by calculating the upper bounds. Consider the allocation of 3 units to subsystem 1. If this is done, no additional redundancy can be applied to subsystems 2 and 3 because all the resources are expended.

If we consider allocations above the minimum bound as incremental policies, $\Delta n_1 = 3$, $\Delta n_2 = 0$, $\Delta n_3 = 0$, or, more compactly, the incremental policy is (3,0,0), and sixteen of the 64 combinations are eliminated. Similar reasoning leads to the conclusion that (2,1,0) and (2,0,1) are allowed policies. Similarly (1,2,0), (1,1,1), and (1,0,2) are possible policies. Lastly, (0,3,0), (0,2,1), (0,1,2), and (0,0,3) are possible solutions for a total of 10 policies to explore. The solutions outlined are clearly displayed by the search tree shown in Figure 5. The branches radiating from the top level node represents the four incremental choices for n_1, and the branches radiating from these four nodes represent the nine possible combinations for n_1 and n_2. The final branches represent the six additional choices that can be made. The numbers at the bottom of each terminating path are the reliabilities achieved by the policy.

Inspection of Figure 5 shows that the optimum incremental policy is (1,1,1) with a reliability of 0.9098 and that the incremen-

tal policy (0,1,2) is a close second with a reliability of 0.9087. Practical considerations that are unstated may make the choice of the second or perhaps third best policy advisable in some cases. This simple example explains the method and illustrates the huge reduction in computational cases due to the lower and upper bounds. It is fairly easy to program the algorithm and a personal computer provides ample computational power even in a large-scale problem.

Conclusion

This article has highlighted some of the more important topics that must be considered in the area of fault-tolerant computing. Because of the complexity of digital systems, many of these techniques must be used in combination to design a highly reliable, highly available complex system.

References

1. Hamming, R.W., *Error Detecting and Correcting Codes*, Bell System Technical Journal, 29 April 1950, pp. 147-160.
2. Shooman, M.L. and C. Marshall, A Mathematical Formulation of Reliability Optimized Design, *Proceedings of 16th IFIP Conference on System Modeling and Optimization*, Compiegne, France, July 5-9, 1993. (Also published in Henry, J. and J.P. Yvon, System Modeling and Optimization, *Lecture Notes in Control and Information Sciences 197*, Springer-Verlag, London, 1994, pp. 941-950.)
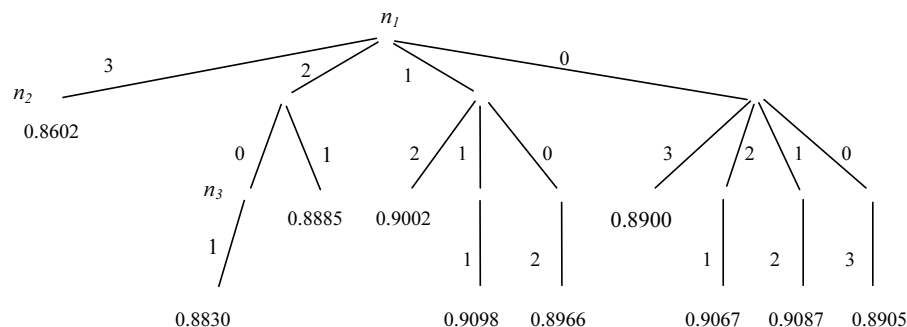
Figure 5. A Search Tree for the Example (Reference 3, Figure 7.6, page 359)

3. Shooman, M.L., *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*, John Wiley, New York, 2002.
4. Siewiorek, D.P. and R.S. Swarz, *Reliable Computer Systems Design and Evaluation*, 3rd ed., A.K. Peters, <www.akpeters.com>, 1998.
5. Wicker, S.B. and V.K. Bhargava, *Reed-Solomon Codes and their Applications*, IEEE Press, New York, 1994.

About the Author

Martin L. Shooman, PhD, is currently President of the consulting firm of Martin L. Shooman & Associates. He served for many years as a Professor of Electrical Engineering and Computer Science at Polytechnic University in Brooklyn, NY. Dr. Shooman has been a Visiting Professor at MIT and Hunter College, and a consultant to Bell Laboratories, NASA, IBM, the U.S. Army, and many other government and commercial organizations. A Fellow of the IEEE, Dr. Shooman has received five Best Paper awards from the IEEE Reliability and Computer Societies. He has contributed to over 100 papers and reports to the research literature, and has given special courses in Britain, Canada, France, Israel, and throughout the U.S.

Dr. Shooman is the author of *Probabilistic Reliability: An Engineering Approach* and *Software Engineering: Design, Reliability, and Management*. His latest book is *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*. Published in January 2002, the book is 552 pages and is priced at $110.00. It can be ordered from the publisher, John Wiley & Sons.

ISBN: 0-471-29342-3
NORTH AMERICA: John Wiley & Sons, Inc.
1-800-225-5945
<custserv@wiley.com>
<www.wiley.com>
REST OF THE WORLD
John Wiley & Sons, Ltd.
+44(0) 1243 779777

RAC Introduces Its *New* Professional Sustainment Program Series

By: Tim Cathcart and Joel Manary

Introduction

Sustainment professionals need a parallel set of skills and tools. One set needs to focus on management aspects of integration of support elements and integration of sustainment issues with other program management functional areas. Numerous training and certification programs address this need. The other set needs to focus on the engineering and other technical aspects of sustainment in a practical and user-oriented fashion. No training and certification in a condensed and user-oriented context has been available.

The Reliability Analysis Center (RAC) has recently developed a new professional certificate program specifically designed for the unique problems currently facing the sustainment community. The Professional Sustainment Program provides the essential technical skills, methods, and tools to implement many new strategies and principles required in economically sustaining an enterprise and the products created by that enterprise.

The Professional Sustainment Program series consist of several courses that comprehensively integrate traditional sustainability analysis and operational effectiveness methodologies with new research findings from several fields of studies, such as supply chain management, integrated lean enterprises, and *e*-logistics.

The Office of the Secretary of Defense has directed all DoD logistic-wide initiatives to adopt commercially "proven" practices and strategies. These logistic transformation objectives include the implementation of many commercial practices such as supply chain management and agile manufacturing and MRO (Maintenance Repair Overhaul) concepts. Many DoD organizations have established transformation offices to implement these new strategies. The organizations using system continue to demand increased attention to sustainment issues affecting systems readiness, and the responsiveness of the logistics infrastructure. The rush to field systems without settling sustainability requirements continues to plague acquisition projects.

Professional Sustainment Program

The Professional Sustainment Program series was developed to provide an educational resource for the sustainment community. It will help them develop the management and technical skills needed to design and implement cost-effective, integrated sustainment networks and agile organizational structures, while still addressing the unique problems facing the sustainment community such as aging systems and providing life cycle support for Commercial-Off-The-Shelf items.

Commercially proven supply chain management and lean enterprise practices have significantly benefited the manufacturing and retail industries but have been difficult to apply in the defense industry because of the high degree of variability in both source material and low volume production requirements.

Under ideal conditions, a sustainment supply chain network would be responsive and flexible enough to meet varying demand conditions. The right types of material and parts would be available in the right quantities, at the right place, at the right time, at an affordable cost. Parts and material shortages coupled with increased maintenance requirements are just some of the issues facing the sustainment community in today's environment. The logistic transformation from a cold war "mass production" operational model into a smaller and more mobile "lean and agile" post cold war operational model will require significant cultural and infrastructure changes.

Reliability Analysis Center's

2003 Training Program

San Diego, CA

March 4-6, 2003

Electronic Design Reliability

Mechanical Design Reliability

Accelerated Testing

RAC

Reliability Analysis Center
201 Mill Street
Rome, NY 13440-6916
Telephone: 888-RAC-USER (722-8737)
315-337-0900
Fax: (315) 337-9932
E-mail: rac@iitri.org
http://rac.iitri.org

Electronic Design Reliability

This intensive course is structured for all key participants in the reliability engineering process. Included are systems and circuit design engineers, quality engineers and members of related disciplines having little or no previous reliability training. The course deals with both theoretical and practical applications of reliability; all considerations related to the design process including parts selection and control, circuit analysis, reliability analysis, reliability test and evaluation, equipment production and usage, reliability-oriented trade-offs, and reliability improvement techniques. Course hand-outs include a course manual and RAC's publication "Reliability Toolkit: Commercial Practices Edition."

Course Instructor

Norman B. Fuqua has 35 years' experience in the reliability-engineering field including teaching reliability techniques and application for the last 20 years. His experience includes the application of reliability on commercial, military and space programs. He holds a BSEE from the University of Illinois, is a senior member of IEEE, and a Registered Professional Engineer. He has published numerous technical papers and has authored two textbooks on equipment reliability and electrostatic discharge. He was responsible for the development of the RAC's "Design Reliability" and "Advanced Design for Reliability" Courses.

Course Contents

General Concepts and Mathematics
1. Definitions
2. Mathematical Foundations
3. Military & International Standards/Handbooks

System Reliability Analysis, Assessment, and Apportionment
1. Allocation/Apportionment
2. Modeling
3. Prediction

Parts Management
1. Part and Vendor Selection
2. Design Criteria and Tools
3. Manufacturing/Assembly Processes

Part Derating and Reliability Prediction
1. Derating Theory
2. Specific Derating Factors for Various Part Types
3. Microcircuit Prediction Example

4. Compare & Contrast: MIL-HDBK-217, Telcordia, PRISM

Reliability Demonstration
1. Statistical Concepts
2. Confidence Intervals
3. QC Concept
4. MIL-STD-781 Methodology

Failure Mode Effects and Criticality Analysis
1. FMECA Characteristics
2. FMEA Methodology
3. CA and RPN Methodologies

Reliability References and Data Sources
1. RAC, GIDEP, NTIS & DTIC
2. Professional Organizations
3. Failure Reporting Analysis and Corrective Action System

Reliability Growth Management
1. The Growth Process
2. Growth Test Planning
3. Duane & AMSAA Plots

Circuit Analysis
1. Circuit Simplification
2. Degradation Analysis Techniques
3. Overstress and Transient Analysis

Fault Tree Analysis
1. Construction Methodology
2. Qualitative Analysis
3. Quantitative Analysis

Design for the Environment
1. Thermal Considerations
2. Shock and Vibration
3. Salt and Humidity
4. EMI & Nuclear Radiation

Reliability Program Management
1. Program Elements
2. Program Implementation
3. Organizational Considerations

Production and Use Reliability and ESS
1. Production Degradation Factors
2. Field Degradation Factors
3. Environmental Stress Screening
4. HALT and HASS

Final Group Problem

Mechanical Design Reliability

This Mechanical Design Reliability Training Course is a practical application of fundamental mechanical engineering to system and component reliability. Designed for the practitioner, this course covers the theories of mechanical reliability and demonstrates the supporting mathematical theory. For the beginner, the essential tools of reliability analysis are presented and demonstrated. These applications are further solidified by practical problem solving and open

discussion. The objective of this extensive application of reliability principles is to leave the participants prepared to address reliability related to mechanical equipment and to provide competency in the predominant tools of mechanical system reliability analysis. Course handouts include a course manual and RAC's publication "Reliability Toolkit: Commercial Practices Edition."

Course Instructor

Ned H. Criscimagna is a Senior Engineer with 37 years experience in engineering, maintenance, and system acquisition. He routinely serves as Project Manager for projects involving reliability and maintainability (R&M) and life cycle cost concerns. In his 20 years as an officer in the US Air Force, he served in a variety of engineering, maintenance, and acquisition positions. He brings to the classroom practical project experience, an appropriate educational background, and an understanding of the product development process. Mr. Criscimagna is the author of many R&M publications and developed a RAC training course on implementing reliability under Defense Acquisition Reform. He received his BSME from the University of Nebraska-Lincoln and his MS in Systems Engineering from the Air Force Institute of Technology. He is an ASQ Certified Reliability Engineer and a SOLE Certified Professional Logistician.

Course Contents

Introduction to Mechanical Design Reliability
1. Scope and Course Content
2. Elements of a Reliability Program
3. Definitions and Terms

Reliability Engineering and Pre-Requisites
1. Part versus System Reliability Issues
2. Probability Functions
   A. Probability Density Functions
   B. Reliability Functions
   C. Hazard Rate Concept
3. Exponential, Normal, Log-normal and Weibull Failure Distributions
4. Choosing the Appropriate Distribution

Reliability Requirements and Goal Setting
1. Deriving Customer Needs and Requirements
2. Determining Product Design Reliability Goals
3. Developing System Reliability Models
4. System Reliability Allocation Methods

Mechanical Reliability Predictions
1. Definitions

2. Mathematical Models
3. Prediction Techniques
   A. Weibull Analysis
      i. Data Requirements
      ii. Mixture of Failure Modes
      iii. Few Failure Times
      iv. Three Parameter Distributions
      v. Plotting Procedures and Interpretation
   B. Empirical Models
      i. Component Models
      ii. S-N Relationships
   C. Mechanical Stress/Strength Interference Method
   D. Cumulative Hazard Rate and Average Failure Rates

System Reliability Analysis
1. Point Process Concept
2. Trend Analysis Techniques
3. Confidence Determination

Failure Modes & Effects Analysis (FMEA)
1. Benefits of Performing an FMEA
2. When is an FMEA Conducted
3. Who Should Perform an FMEA
4. Prerequisites and Procedures of Performing an FMEA
5. Failure Mode, Effects and Criticality Analysis (FMECA)

Fault Tree Analysis (FTA)
1. Benefits of Performing an FTA
2. Appropriate Applications of an FTA
3. FTA Procedures
4. Logic Symbols
5. Construction Rules
6. Qualitative and Quantitative Analysis

Reliability Testing
1. Reliability Growth Testing
   A. Duane Model
   B. Crow-AMSAA Model
2. Part Testing Procedures
3. Accelerated Life Testing
4. Reliability Qualification Testing
5. Production Reliability Acceptance Testing

Maintaining a Reliable Design
1. Addressing Vendor Issues
2. Reliability Information Systems
3. Developing Preventive Maintenance Programs

Review and Wrap-Up
1. Review and Reliability Program Elements and Correct Timing of Analysis
2. Specific Key Points of Each Analysis
3. Key Elements to be Addressed at Various Design Reviews
4. Importance of Utilizing and Contributing to a Reliability Information System
5. Where Do You Go From Here?

Accelerated Testing

This results-oriented course provides both an in-depth introduction to the underlying statistical theory and methods as well as a complete overview and step-by-step guidance on practical applications of the learned theory using ReliaSoft's ALTA, a software tool designed expressly for the analysis of accelerated life test data. The first half of the course presents the theory and required background while the latter half concentrates on practical applications. The practical application portion of the seminar involves exploration and interactive hands-on learning (using PC's and software) to complement and enhance the attendee's knowledge in the subject of Accelerated Life Testing. This integrated presentation of both the underlying theories and the software will enable the attendee to quickly and easily apply the learned concepts and methods in the workplace. Each student will receive a course manual and ReliaSoft's ALTA software package, which is a $995 value.

Course Instructor
Mr. Pantelis Vassiliou is the President of ReliaSoft Corporation, a research and development organization comprised of reliability engineers, statisticians and computer scientists, and dedicated to providing reliability-engineering solutions. For the past seven years, Mr. Vassiliou has managed and coordinated ReliaSoft's R&D efforts to deliver state of the art software tools and reference books for applying reliability engineering concepts and methodologies. This includes ReliaSoft's ALTA and "ReliaSoft's Accelerated Testing Reference," the first commercial software package specifically designed for analyzing accelerated life data. Mr. Vassiliou has presented lecturers and training seminars in Reliability Engineering and Life Data Analysis worldwide. He holds a Masters degree from the University of Arizona in Reliability Engineering.

Course Contents
Introduction Background and Overview
1. Overview of Reliability Engineering and Life Data Analysis
2. Statistical theory and applications
3. Most commonly used distributions for product life, and their applications
4. Product life data types and censoring schemes

5. Parameter estimation methods
6. Confidence Bounds

Accelerated Life Testing Theory Overview
1. Overview of Accelerated Tests
2. Types of Accelerated Tests
3. Accelerated Life Testing and How it is Applied
4. Overview of Stress Loading Models and Analysis
5. Applicable Stress-Life Relationship Models and Their Analyses
   A. Arrhenius Relationship
   B. Eyring Relationship
   C. Inverse Power Relationship
   D. Temperature - Humidity Relationship
   E. Temperature - Non-thermal Relationship
   F. Proportional Hazards Model
   G. Non-Proportional Hazards Model
   H. Cumulative Exposure/Damage Model (Step-Stress)
6. Predicting Reliabilities, Warranty Times and MTTF (MTBF) using accelerated life data
7. Looking at Accelerated Life Plots
   A. Probability Plots
   B. Reliability Plots
   C. Probability Density Function Plots
   D. Life-Stress Plots
   E. Acceleration Factor Plots
8. Confidence Bounds on accelerated life data
9. Examples and Case Studies

Application of Accelerated Life Data Analysis Theory (Hands-on using computers and software)
1. Overview of ALTA
2. Applying previously presented theory utilizing ALTA
   A. Entering and analyzing data with different censoring schemes
   B. Available statistical distributions and Stress-Life relationships
   C. Probability Plots, creating & using
   D. Life-Stress Plots, creating & using
   E. Looking at other plots; pdf, Reliability, Failure Rate, Acceleration Factor, etc.
   F. Looking at 3D plots, creating and interpreting
   G. Using Confidence Bounds
3. Illustrating ALTA using real life examples
4. Examples and Case Studies
5. Hands-on Session Using ReliaSoft's ALTA

RAC'S 2003 Training Program
Registration Form
San Diego, CA

Please select one course & check box accordingly

☐ Electronic Design Reliability $ 1,095
☐ Mechanical Design Reliability $ 1,095
☐ Accelerated Testing $ 1,695*

*Includes a copy of ReliaSoft Alta Software
2.1 CEUs will be earned for each course.
Attendees are encouraged to bring their own calculator.

RAC Training Course Details

Course Dates	March 4-6, 2003
Course Registration Deadline	February 14, 2003
Course Site	Knowledge Development Centers (KDC)
	401 B Street, Suite 650
	San Diego, CA 92101
	(619) 235-8600

Lodging: KDC facilities are non-residential which allows the attendee to choose their own overnight accommodations. A large variety of hotels to meet your individual needs are conveniently located within a short distance of Knowledge Development Center's world class training facility. Course attendees are responsible for making their own hotel reservations and are encouraged to do this soon. Knowledge Development Centers has negotiated special rates with six area hotels. For details please visit http://www.kdc-sd.com/hotels.htm.

Enrollment Information

Registration: Complete the registration form in this flyer and mail with your check or purchase order to the Reliability Analysis Center. We urge you to register as soon as possible, as class size is limited to 24. The fee includes attendance at one of the 3-day basic courses of the students choice, handout materials and coffee breaks. Hotels and meals are not included.

Multiple-Attendance Discounts: The discount schedule for course attendance by several persons from one corporate entity is:

No. of Attendees	% Discount
1-2	None
3-4	10%
5 and above	20%

Refunds: Cancellations received up to five working days before the courses begin are refundable. After that, cancellations are subject to the entire registration fee, which you may apply toward a future course. Please note that if you don't cancel and don't attend you are still responsible for payment. Substitutes may be made at any time.

Instruction Periods: Registration will be March 4th at 7:30 a.m. Classes run from 8:00 a.m. to 4:00 p.m. daily.

Additional Information: We reserve the right to cancel or postpone any of the training courses one week prior to the start of the course. For further information contact the Reliability Analysis Center at (888) RAC-USER (722-8737) or (315) 337-0900, FAX: (315) 337-9932.

Course Registration Only

Name _____

Company _____

Address _____

City _____ State _____ Zip _____ Country _____

Phone _____ Ext _____ Fax _____

E-mail _____

Method of Payment:
☐ Company/ Personal Check Enclosed (Make checks payable to IITRI/RAC)

☐ Credit card #: _____ Exp Date: _____

     Type (circle):   *American Express*   *VISA*   *Mastercard*

Name on Card _____

Signature _____

Billing Address _____

Federal ID No.: 36-2169122

Please list additional registrations on a separate sheet and attach.

Mail to Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916 or Fax to (315) 337-9932.

The RAC is actively researching many of these problems and investigating the application of new technologies and strategies that could be leveraged in providing affordable products and sustainment networks. The courses are structured to provide a complete life cycle perspective of sustainment. Lean Enterprise principles and transformation leadership is incorporated in the series to help organization implement and sustain a "lean enterprise" approach organizational improvement efforts.

Course Descriptions

Four courses are available. The Professional Sustainment Certificate requires that students complete the last three courses from the Professional Sustainment Program Series.

Course Overview Sustainment Principles and Strategies. This 3-day course provides an executive overview of systems sustainment and integrates systems engineering principles with proven commercial business practices and strategies used today in industry. New sustainment approaches for commercial off-the-shelf intensive systems are presented and evaluated through group case study discussions. New logistics technologies, tools, and application software systems are also explored. Several case studies are used to illustrate critical principles and practices for system sustainment analysis, design, and implementation.

Sustainment Analysis and Life Cycle Management: Principles and Applications. This 3-day course presents system engineering and sustainability analysis methodologies and strategies required to design, produce, operate, and maintain a cost-effective system. Initial focus is on needs identification and problem definition. It then moves into systems engineering synthesis, functional analysis, and evaluation activities during the complete life cycle from conceptual and preliminary system design phases to deployment and sustainment. The course treats sustainability attributes such as maintainability, manufacturability, and affordability, as part of the systems engineering process. This course provides the participant with the tools and techniques that can be used through the life cycle from the perspective of system sustainment.

Supply Chain Design and Logistics Operations Management: Integrating the Sustainment Network. This 3-day course presents the theory and practice of the core functions of the enterprise that impact the supply chain management and operational logistic support of fielded systems. It provides a basic understanding of strategy, organizational structure and behavior for an "integrated sustainment enterprises network" based upon its design and operation. Recent research results from several fields of study such as supply chain management, integrated lean enterprises, and *e*-logistics are presented. New logistic technologies, tools and application software systems are also explored. This course provides the participant with the tools and techniques needed to design, implement, and operate effective sustainment enterprise supply chain and support services.

Lean Enterprise Principles and Transformation Leadership. This 3-day course provides a comprehensive overview on lean principles and practices, and provides a new framework in defining a lean enterprise. Lean means adding value by eliminating waste, being responsive to change, focusing on quality, and enhancing the effectiveness of the enterprise. Lean enterprise implementation and assessment is presented using a lean enterprise model developed by the Massachusetts Institute of Technology (MIT). Many of the principles and strategies presented in the course are based upon extensive research conducted in MIT's International Motor Vehicle Program and Lean Aerospace Initiative. The course covers the lean philosophy in-depth along with the key supporting tools and practices for successful lean enterprise transformation. The course analyzes lean transformation unique issues applicable to both sustainment organizations and extended networks.

For further information contact the RAC or Joel Manary, RAC course presenter, at: <manaryj@cox.net>, (619) 524-3945.

Program Managers Handbook -- Common Practices to Mitigate the Risk of Obsolescence

By: Walter Tomczykowski – ARINC Engineering Services, LLC

Abstract

ARINC, under contract GS-35F-4825G, task order DMEA90-99-F-A0013, with the Defense Microelectronics Activity (DMEA), documented common practices for minimizing the risk of obsolescence into a program manager's handbook.

This article describes The Program Managers Handbook—Common Practices to Mitigate the Risk of Obsolescence, which provides practices and a list of resources that other program managers have used to minimize the impacts and cost of obsolescence. The primary audience for this handbook is a program manager who has been recently introduced to DMSMS. The common practices in this handbook can be implemented to minimize the impact of DMSMS.

Introduction

The Department of Defense (DoD) defines obsolescence as diminishing manufacturing sources and material shortages (DMSMS). DMSMS is a serious issue for the DoD, the airline community, and many commercial industries. Due to rapid advances in semiconductor technology, microelectronic component life cycles have been shortened from between 3 and 5 years to 18 [1] months. The average DoD system acquisition life cycle time (measured from program start to initial operating capability) is 132 months [2]. Semiconductor technology could change over seven times during this acquisition cycle which could cause significant risk that components selected during system development and demonstration might be obsolete before initial operating capability or sooner.

The Defense Microelectronics Activity (DMEA), DoD Executive Agent for Microelectronics DMSMS operates under the authority, direction, and control of the Deputy Under Secretary of Defense for Logistics & Material Readiness. Its primary mission is to leverage the capabilities and advantages of advanced technology to solve operational problems in existing weapon systems, increase operational capabilities, reduce operating and support costs, and reduce the effects of DMSMS. In this capacity, DMEA collected the common practices used today for minimizing the risk of obsolescence.

Minimizing the impact of component (parts) obsolescence and technical obsolescence risk is the heart of the DMSMS concern. The *Program Managers Handbook—Common Practices to Mitigate the Risk of Obsolescence—*provides the practices and a list of resources that program managers have used to minimize the impacts and cost of obsolescence. DMEA is in the process of converting this document into a Military Handbook. The Military Handbook is planned for completion in the spring of 2003. This article provides a summary of these practices.

The primary audience for this handbook is a program manager who has been recently introduced to DMSMS. The handbook complements the commonly used resolution guides—the Naval Sea Systems Command *Case Resolution Procedures Guide*, the Air Force Materiel Command *DMSMS Program Case Resolution Guide,* and the Army Materiel Command *DMSMS Case Resolution Guide*. This handbook provides the program manager a shopping list of common practices and resources that should be implemented to minimize the impact of DMSMS. Many experienced program managers from both DoD and industry have indicated that it is also necessary to provide guidance on how and when to incorporate these obsolescence risk mitigation strategies into contractual language [3].

Handbook Content

The Program Managers Handbook provides three intensity levels of common practices that include activities that could be implemented to mitigate the risk of DMSMS:

- Level 1—Practices are implemented to resolve current obsolete items. Some of these activities may be considered reactive.
- Level 2—Minimal required practices are needed to mitigate the risk of future obsolete items. The majority of these activities are perceived as proactive.

- Level 3—Advanced practices are required to mitigate the risk of obsolescence when there is a high opportunity to enhance supportability or reduce total cost of ownership. These activities are proactive and may require additional program funding.

Selecting a practice is influenced by the resources available to manage DMSMS, the life cycle phase, senior management philosophy, and program complexity. The practices associated with these levels form the basis of a DMSMS program that can be implemented to mitigate the impact of DMSMS. Although an expense is associated with the implementation of a DMSMS program, cost avoidance can be realized from such a program. A list of the practices for each level is presented in Table 1. An event usually occurs that convinces the program manager that one or more practices need to be implemented. These events are called *triggers*.

The relative implementation cost versus potential for Total Ownership Cost (TOC) reduction, along with a summary of the possible triggers, is shown in Figure 1. Business case analyses from the B-2, AEGIS, and Joint Stars programs have shown that the implementation of these practices can result in lowering the cost of resolving obsolescence problems and reducing TOC. It is important to note that as more practices are selected, the potential for reduction of TOC increases.

The draft Program Managers Handbook contains detailed descriptions of each practice and can be obtained at <http://www.dmea.osd.mil>. These practices will be updated and new practices will be added when the Military Handbook is completed. New practices under consideration for the Military Handbook include the following:

- Create an integrated product team including suppliers and end users (System Program Office DMSMS Management Activity)
- Incorporate availability guarantees in contracts
- Implement open systems architecture (OSA) interface standards
- Plan for periodic replacement (i.e., technology insertion or technology refresh)
- Implement design guidelines
  - Select parts relatively new into their life cycles
  - Use modular systems
  - Compile software independent of the target

Table 1. Common Practices

Level 1	Level 2	Level 3
• DMSMS Focal Point	• Awareness Training	• Circuit Design
• Awareness Briefing	• DMSMS Prediction	• VHDL
• Internal Communications	• DMSMS Steering Group	• Technology Assessment
• External Communications	• COTS List	• Electronic Data Interchange
• DMSMS Plan	• DMSMS Solution Database	(EDI)
• Parts List Screening	• Opportunity Index	• Technology Insertion
• Parts List Monitoring	• Web Site	
• Resolution of Current Items		
• Supportability Checklist		

Note: The selection of any of the possible practices are influenced by the triggers and one or more of the following:

- Program complexity
- Available resources
- Management philosophy
- Stage in life cycle

Level 3

Circuit design guidelines
VHDL
Technology assessment
EDI
Technology insertion

Level 2

Awareness training
DMSMS prediction
DMSMS steering group
COTS list
DMSMS solution database
Opportunity index
Web site

Level 1

DMSMS focal point
Awareness briefing
Internal communications
External communications
DMSMS plan
Parts list screening
Parts list monitoring
Resolution of current items
Supportability checklist

Possible Practices

Relative Implementation Cost — High / Low

Low	Potential for TOC Reduction	High

Possible Triggers

Level	Level	Level
Initial DMSMS awareness by program manager (PM) <10% of parts unsupportable <10 years remaining in system life cycle	Increased awareness from PM 10-20% of parts unsupportable 10-20 years remaining in system life cycle	Higher management (above PM) awareness of supportability problems >20% of parts unsupportable >20 years remaining in system life cycle Opportunity to enhance supportability or reduce total cost of ownership

Figure 1. Stepping up to Minimize the Risk of Parts Obsolescence (ARINC 2000)

Acknowledgment

References

1. The 18 months is based on Moore's Law, which states that the density of components (e.g., fabrication process minimum feature size measured in micrometers) doubles about every 18 months.
2. The historical baseline is 132 months. The current DoD goal is to reduce this by 25% to 99 months.
3. DMSMS Acquisition Guidelines have been published by DMEA and can be obtained from the DMEA web site <http://www.dmea.osd.mil>.

About the Author

Walter Tomczykowski is the DMSMS Program Director at ARINC. He received an MS in Reliability Engineering from the University of Maryland. For the last 20 years he has been performing product support work in the areas of reliability, maintainability, and obsolescence management for a variety of Air Force, Navy, and Army programs. Currently he provides DMSMS support to DMEA, the NAVAIR Aging Aircraft IPT, and the JTIDS program office. He is the author of the DMEA DMSMS Cost Factors, the DMSMS Program Managers Handbook, and the DMSMS Acquisition Guidelines. Previously his work in reliability has been published in the "Wiley Encyclopedia of Electrical and Electronics Engineering" and the "Product Reliability, Maintainability, and Supportability Handbook." Walter is an ASQ Certified Reliability Engineer and Certified Quality Auditor.

Walter J. Tomczykowski
ARINC Engineering Services, LLC
2551 Riva Road
Annapolis, MD 21401
E-mail: <wtomczyk@arinc.com>

Do it right,

or don't

do it at all...

ISTFA 2003 • Call for Papers

29th International Symposium for Testing and Failure Analysis
3-7 November 2003 • Santa Clara Convention Center • Santa Clara, California USA
Sponsored by: ASM Electronic Device Failure Analysis Society (EDFAS)

ISTFA 2003 is soliciting <u>original, previously unpublished</u> papers on a wide range of Testing and Failure Analysis topics of practical value to anyone working to detect, understand and eliminate electronic device and system failures. Non-commercial papers from equipment vendors dealing with new or unique tools and methodologies, applications and results are welcome. Papers will be selected for inclusion in the technical program on the basis of appropriateness and quality of data, technical importance, novelty/originality, and interpretation of results. <u>Paper acceptance is based entirely on the information included in the abstract</u>. We are currently seeking abstracts on (but not limited to) the following relevant topics*:

- Advanced Techniques
- Sample Preparation
- Die Level Fault Isolation
- Yield Enhancement
- Failure Analysis Process
- System Level Analysis
- Package Level Analysis
- Optoelectronic Devices
- Optical Probing and Emission
- FIB for Fault Isolation and Design/Edit
- Discretes and Passives
- Metrology & Materials Analysis
- Test
- SPM Techniques
- MEMS
- Military

CALL FOR PAPERS DEADLINE ▪ 3 March 2003

Abstract Submission: ISTFA 2003 will consider abstracts in English only (two-page minimum) including representative images, figures, and references. It is highly advisable to include sufficient detail to allow for fair evaluation of the work discussed. Also, include the following information for all authors, presenting author listed first: complete name, title, affiliation with complete mailing address, telephone and fax numbers, and E-mail address. This information must be included with the abstract or it will not be considered for evaluation. **Please go to <www.edfas.org/istfa> to submit your abstract. The deadline for final submission is 3 March 2003.**

Manuscript Submission: All authors accepted into the ISTFA 2003 Symposium are required to submit a full manuscript for review by 14 July 2003. A final manuscript for publication will be required in electronic format by 18 August 2003.

Pre-approval to present your work at ISTFA 2003 is recommended. All costs associated with your attendance will be at your expense (travel, housing, registration).

*For information on ISTFA 2003, session topic descriptions, and information regarding abstract submission, please contact the ISTFA Conference Administrator, ASM International, Materials Park, Ohio 44073-0002 (440) 338-5151 or visit the ISTFA web site at <www.edfas.org/istfa>.

System Safety Conference

For obvious reasons, most of the articles and calendar entries for the RAC Journal deal with reliability and maintainability. Over the past year or so, we have endeavored to increase our coverage of supportability and quality. Another topic, closely related to reliability, is system safety. Not only is the probability and consequences of failure of equal concern to both the safety and reliability engineer, many of the analyses are similar and mutually supportive.

As a first step in emphasizing the importance of safety and its close relationship to reliability, we note that the System Safety Society will be holding its 21st International System Safety Conference, August 4-8, 2003, in Ottawa, Ontario, Canada. This conference is an international forum for the technical presentation and discussion of all aspects and issues regarding system safety engineering and management.

The theme of this year's conference is Broader Perspectives, Focused Solutions. The emphasis of the conference activities is on the knowledge and skills necessary to create the system safety solutions for increasingly complex technologies and missions. The spectrum of topics will cover both the art and science of system safety, as well as the organizational issues influencing the effective management of system safety in the product life cycle. This conference is the major forum for system safety and related professionals, and features a week of technical sessions, tutorials, workshops, special events, social affairs, luncheons, and the society's awards banquet. The conference proceedings are the premier collection of work in the system safety field.

For additional information, contact:

Gerry Einarsson, Conference Chair
24 Wedgewood Cres.
Ottawa, ON Canada K1B 4B4
Tel: (613) 824-2468
E-mail: <einargk@rogers.com>
On the Web: <http://www.system-safety.org>

item
S o f t w a r e

PUTTING THE PIECES OF RELIABILITY, AVAILABILITY,
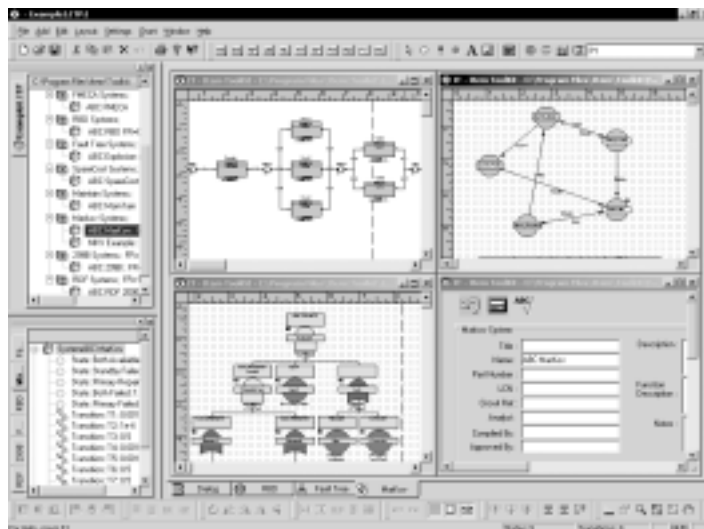MAINTAINABILITY, SAFETY AND QUALITY ASSURANCE TOGETHER

YOU ASKED, AND WE LISTENED

New Analysis Modules!

ITEM TOOLKIT MODULES
- MIL-217 Reliability Prediction
- Bellcore/Telcordia Reliability Prediction
- **NEW!** 299B Reliability Prediction
- **NEW!** RDF Reliability Prediction
- NSWC Mechanical Reliability Prediction
- **NEW!** Maintainability Analysis
- Failure Mode, Effects and Criticality Analysis
- Reliability Block Diagram
- Fault Tree Analysis
- **NEW!** Markov Analysis
- **NEW!** SpareCost Analysis

ITEM QA MODULES
- Design FMEA
- Process FMEA
- Control Plan
- **NEW!** Document Control and Audit (DCA)
- **NEW!** Calibration Analysis
- **NEW!** Concern and Corrective Action Management (CCAR)
- **NEW!** Statistical Process Control (SPC)

Item Software (USA) Inc.
2190 Towne Centre Place, Suite 314, Anaheim, CA 92806
Tel: 714-935-2900 - Fax: 714-935-2911
URL: www.itemsoft.com
E-mail: itemusa@itemsoft.com

Item Software (UK) Limited
1 Manor Court, Barnes Wallis Road, Fareham, Hampshire -
PO15 15TH, U.K.
Tel: +44 (0) 1489 885085 - Fax: +44 (0) 1489 885065
E-mail: sales@itemuk.com

**Visit our Web site at www.itemsoft.com,
or call us today for a free demo CD and product catalog.**

PRISM Column

Meet the PRISM Team

Beginning with this issue, the RAC Journal will include a column that addresses techniques and advice on the use of PRISM. Information presented will be in response to inquiries, comments, and suggestions made by our users. However, our first column familiarizes readers with the RAC PRISM team.

The PRISM team is committed to providing the user community with a high quality reliability prediction tool and the training to assist users in its application. This team has been responsible for developing, releasing, and supporting the tool since January of 2000. Using feedback provided by users, this core group has continuously improved the quality and usability of this tool and its interface.

D. David Dylis – Project Manager. Dave is responsible for coordinating the team's efforts in development and customer support. As technical lead, he is responsible for addressing PRISM technical inquiries, methodology modifications, and PRISM forum questions. He is responsible for establishing PRISM reseller agreements and site licenses. He has authored and co-authored numerous technical papers and has presented the PRISM methodology at conferences and meetings internationally. Dave has 22 years experience in reliability techniques and applications and uses PRISM to perform predictions for clients. He is an ASQC Certified Reliability Engineer and holds a BS degree in Chemistry and Physics from Utica College of Syracuse University.

Tammy T. Sehn – Lead Programmer. Tammy is responsible for all aspects of the development and maintenance of the software. She answers all software-related technical inquiries and assists users in installing the software. In addition to these duties, Tammy works on software documentation, including the PRISM User and Training Manuals. Tammy has a BS degree in Information Science from Hartwick College.

Norman B. Fuqua – PRISM Instructor. Norm is responsible for the development and maintenance of the PRISM training program and manual. Drawing on his 38 years of experience and 22 years of teaching reliability techniques and applications, he developed a "hands-on" interactive training course. He assists in reviewing and testing the software. He is also familiar with various reliability methodologies and regularly uses PRISM to perform predictions for clients. Norm holds a BSEE from the University of Illinois, is a Senior Member of IEEE, and is a Registered Professional Engineer.

Nathan D. Holzhauer – PRISM Instructor. Nathan is responsible for assisting with the maintenance of the PRISM training program and has five years teaching experience. He supports ongoing PRISM development as an in house beta tester and assists in the software review and testing processes. He is also familiar with various reliability methodologies and regularly uses PRISM to perform predictions for clients. He holds a BS degree in Engineering Physics from St. Bonaventure University.

Adrian Piaschyk – PRISM Tester. Adrian is responsible for beta testing of PRISM. This rigorous testing of the user interface and the associated functionalities helps assure the release of a quality product. As a user and tester for PRISM Adrian offers valuable feedback on the product's current configuration and recommends improvements for future versions. He is also familiar with various reliability methodologies and regularly uses PRISM to perform predictions for clients. He holds a BS degree in Electrical Engineering from the University of Rochester.

While this is the core team, every member of the RAC staff strives to provide users the best technical support in Reliability, Maintainability, Supportability, and Quality and the PRISM methodology. Dave, Tammy, Norm, Nathan, and Adrian are available to answer all your concerns and questions. Feel free to contact them at any time using the PRISM forum at <http://rac.iitri.org/prism>, by phone at (315) 339-7055, or E-mailing them at <rac_software@iitri.org>.

Adrian Piaschyk, Tammy Sehn, Norman Fuqua, Nathan Holzhauer, D. David Dylis

item
S o f t w a r e

PUTTING THE PIECES OF RELIABILITY, AVAILABILITY,
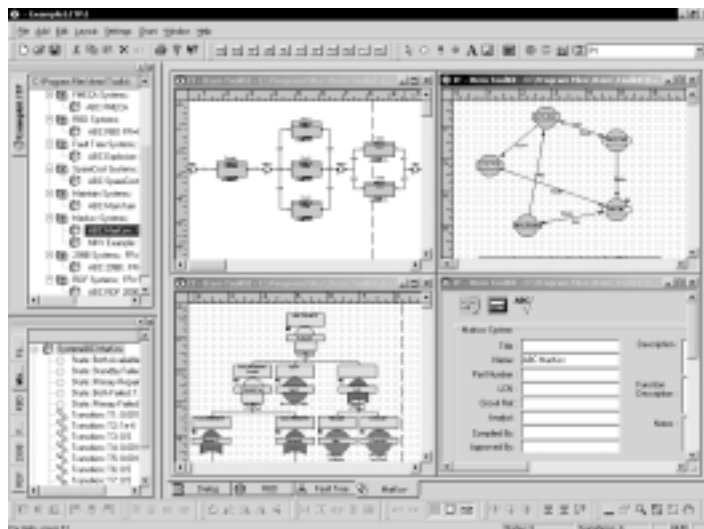MAINTAINABILITY, SAFETY AND QUALITY ASSURANCE TOGETHER

YOU ASKED, AND WE LISTENED

New Analysis Modules!

ITEM TOOLKIT MODULES
- ■ MIL-217 Reliability Prediction
- ■ Bellcore/Telcordia Reliability Prediction
- **NEW!** ■ 299B Reliability Prediction
- **NEW!** ■ RDF Reliability Prediction
- ■ NSWC Mechanical Reliability Prediction
- **NEW!** ■ Maintainability Analysis
- ■ Failure Mode, Effects and Criticality Analysis
- ■ Reliability Block Diagram
- ■ Fault Tree Analysis
- **NEW!** ■ Markov Analysis
- **NEW!** ■ SpareCost Analysis

ITEM QA MODULES
- ■ Design FMEA
- ■ Process FMEA
- ■ Control Plan
- **NEW!** ■ Document Control and Audit (DCA)
- **NEW!** ■ Calibration Analysis
- **NEW!** ■ Concern and Corrective Action
  Management (CCAR)
- **NEW!** ■ Statistical Process Control (SPC)

Item Software (USA) Inc.
2190 Towne Centre Place, Suite 314, Anaheim, CA 92806
Tel: 714-935-2900 - Fax: 714-935-2911
URL: www.itemsoft.com
E-mail: itemusa@itemsoft.com

Item Software (UK) Limited
1 Manor Court, Barnes Wallis Road, Fareham, Hampshire -
PO15 15TH, U.K.
Tel: +44 (0) 1489 885085 - Fax: +44 (0) 1489 885065
E-mail: sales@itemuk.com

Visit our Web site at www.itemsoft.com,
or call us today for a free demo CD and product catalog.

Future Events in Reliability, Maintainability, Quality & Supportability

International IEEE Conference - Electronic Product Reliability & Liability
January 13-17, 2003
Hong Kong and Shenzhen, China
Contact: Angie Wong, Secretariat, Int'l IEEE Conference
City University of Hong Kong
EPA Centre
Department of Electronic Engineering
83 Tat Chee Avenue
Hong Kong, China
Tel: (852) 2788 7379
Fax: (852) 2788 7579
E-mail: <wywong@ee.cityu.edu.hk>
On the Web: <http://http://www.calce.umd.edu/whats_new/upcoming/2002/HK_regis.pdf>

The Annual Reliability and Maintainability Symposium (RAMS 2003)
January 27-30, 2003
Tampa, FL
Contact: Dr. John English, General Chair
University of Arkansas
Department of Industrial Engineering
4207 Bell Engineering Center
Fayetteville, AK 72701
Tel: (479) 575-6029
E-mail: <chair@rams.org>
On the Web: <http://www.rams.org>

Commercialization of Military & Space Electronics
February 10-13, 2003
Los Angeles, CA
Contact: Dale Stamps or Leon Hamiter
Composites Technology, Inc.
Huntsville, AL 35801
Tel: (256) 536-1304
Fax: (256) 539-8477
E-mail: <dale@cti-us.com> or <lhamiter@cti-us.com>
On the Web: <http://www.cti-us.com>

SAE 2003
March 3-6, 2003
Detroit, MI
Contact: SAE
400 Commonwealth Drive
Warrendale, PA 15096-0001
Tel: (724) 776-4841
Fax: (724) 776-0790
E-mail: <custsvc@sae.org>
On the Web: <http://www.sae.org/congress>

NDIA Science & Technology Conference/ DoD Tech Exposition
March 4-6, 2003
Charleston, SC
Contact: Tim Becker
NDIA
2111 Wilson Blvd., Suite 400
Arlington, VA 22201
Tel: (703) 247-2573
Fax: (703) 522-1885
E-mail: <tbecker@ndia.org>
On the Web: <http://register.ndia.org/interview/register.ndia?PID=Brochure&SID>

Conference on Systems Integration (CSI)
March 12-14, 2003
Hoboken, NJ
Contact: Dr. Dinesh Verma
Associate Dean and Professor of Systems Engineering
School of Engineering
Stevens Institute of Technology
Hoboken, NJ 07030
Tel: (201) 216-8334
Fax: (201) 216-8645
E-mail: <dverma@stevens-tech.edu>
On the Web: <http://attila.stevens-tech.edu/seem/>

Corrosion 2003
March 16-20, 2003
San Diego, CA
Contact: Cindy Euton
NACE International
Tel: (281) 228-6274
Fax: (281) 228-6374
E-mail: <cindy.euton@mail.nace.org>
On the Web: <http://nace.org/nace/content/Conferences/c2003/welcome.asp>

IEEE International Reliability Physics Symposium
March 30 - April 3, 2003
Dallas, TX
Contact: Timothy A. Rost
Texas Instruments, MS 3737
13560 N. Central Expressway
Dallas, TX 75243 USA
Tel: (972) 995-9035
Fax: (972) 995-5013
E-mail: <t-rost@ti.com>
On the Web: <http://www.irps.org>

Also visit our Calendar web page at <http://rac.iitri.org/NewsAndEvents/rac_calendar.html>

5th Annual Mid-Atlantic Logistics
April 3-5, 2003
Williamsburg, VA
Contact: John H. Davids
Northrup Grumman
Tel: (410) 993-8172
Fax: (410) 694-2076
E-mail: <john_h_davids@mail.northgrum>
On the Web: <http://www.mid-atlantic-log.org>

The Military & Aerospace Electronics East 2003 Show with COTScon
April 23-24, 2003
Baltimore, MD
Contact: Maureen Kane
98 Spit Brook Road
Nashua, NH 03062-5737
Tel: (603) 891-9423
Fax: (603) 891-9490
E-mail: <maureenk@pennwell.com>
On the Web: <http://mae.pennnet.com/Events/MAE/cots/EAST03/cots_east_general.cfm>

Software Technology Conference
April 28 – May 1, 2003
Salt Lake City, UT
Contact: Lee Ann Ferrara, Conf & Event Info
Utah State University
Logan, UT 84322-5045
Tel: (435) 797-7042
Fax: (435) 797-0861
E-mail: <leeannf@ext.usu.edu>
On the Web: <http://www.stc-online.org>

Intl Conference of Maintenance Societies (ICOMS-2003)
May 28-30, 2003
Contact: Sally Nugent
ICOMS
P.O. Box 634
Brentford Square
Victoria 3131, Australia
Tel: 61(0)3 9874 0800
Fax: 61(0)3 9874 4800
E-mail: <icoms@corrprev.org.au>
On the Web: <http://www.mesa.org.au>

From the Editor

Probability and Statistics – Allies or Foes of the Reliability Engineer?

I earned my Master's Degree in Systems Engineering, with a focus in reliability, from the Air Force Institute of Technology at Wright-Patterson Air Force Base, OH. The required courses included probability and statistics courses. These were new areas of study for me. I had taken many mathematics courses in undergraduate school, but none in probability and statistics. Evidently, those who developed the curriculum for undergraduate students in mechanical engineering did not believe that probability and statistics were needed.

Unlike the manner in which the proverbial duck takes to water, I did not particularly like probability and statistics. I was suspicious of any branch of mathematics that talks about an expected value with zero probability (the expected value of rolling an honest die, for example)! I was bemused by the statistician's obsession with stating things just so. Thus, we can say that there is a probability that a given interval contains the true statistic in question – we must never say that there is a probability that the given statistic in question is included in the interval. It's either in the interval or it isn't. Such statistical proprieties were lost on me at the time.

Today, I have a better regard for the importance of probability and statistics. Much of it still mystifies me and I would be the last person to claim to be an expert; I most certainly am not a statistician. Over the years, however, I have come to appreciate how little in this universe is truly deterministic.

In the early 1960s, when I was in undergraduate school, we were not taught anything but deterministic methods. Materials had a certain strength. If they were placed under a given load, you always used a maximum point value, you could calculate the factor, or margin, of safety. Probabilistic methods were in their infancy at that time. By the time I was in graduate school, we learned about them using a text titled "Probabilistic Approaches to Design" by Edward Haugen. Today, probabilistic methods are widely used in engineering and in areas such as risk management.

Reliability, I believe, got a bad reputation, especially within NASA, in the early '60s due to being confused with probability and statistics. Instead of reliability being advanced as an engineering discipline, it became almost synonymous with predictions. According to an old anecdote (I have no idea if it's true), statisticians told NASA that the Apollo project was impossible. They developed a reliability model for the entire system: the Saturn launch vehicle, the command and service modules, and the lunar lander. Based on the sheer number of parts, they predicted a reliability number so low that failure was almost certain. This answer was unacceptable to NASA. So "reliability" was replaced with exhaustive testing, incredible attention to manufacturing and assembly, and extensive use of sensors and safeguards.

If the anecdote is true, it reflects a common misconception about reliability. Reliability engineering is not equivalent to probability and statistics or vice versa. One would never equate mechanical engineering with calculus – mathematics only provides the basis for measurement in engineering. To quote William Thomson, Lord Kelvin, "When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science."

Ned H. Criscimagna

Probability and statistics constitute the mathematics of reliability engineering. They allow us to express our discipline in numbers, thereby making a science of what would otherwise be "opinion." But, they do not constitute the whole of reliability engineering. Far from it. Few would expect a mathematician to design an aircraft. Why, then, should we expect a statistician to design a reliable product?

Reliability is and will always be the purview of engineers. For this reason, it is somewhat disconcerting to realize that most graduating engineers have never heard of reliability, or have received only a brief introduction to the discipline. Many have never taken a focused course in probability and statistics. Given the already heavy load of courses most undergraduate engineering students must take, these shortcomings are understandable but still regrettable. If they are fortunate, engineers will be given the opportunity to take courses after being hired and given the assignment of being "the reliability engineer."

The title of this little piece is "Probability and Statistics – Ally or Foe of the Reliability Engineer?". So which is it? If we keep the role of probability and statistics in reliability engineering in perspective, they are definitely our allies. It is only when we forget that reliability is an engineering discipline that they can become our foes.

RAC

Order Form

Call:	(888) RAC - USER		Reliability Analysis Center
	(315) 337 - 0900		201 Mill Street
Fax:	(315) 337 - 9932		Rome, NY 13440-6916
Web:	http://rac.iitri.org		E-mail: rac@iitri.org

Quantity	Title*	US Price Each	Non-US Price	Total
	Quality Toolkit	$50.00	$60.00	
	Maintainability Toolkit	$50.00	$60.00	
	PRISM	$1995.00	$2195.00	
	A Practical Guide to Developing Rel. Human-Machine Sys. & Proc.	$75.00	$85.00	
	Electronic Derating for Optimum Performance	$75.00	$85.00	
Shipping and Handling: US Orders add $6.00 per book or CD-ROM for First Class ($10.00 for NPRD or VZAP, $14.00 for EPRD, $2.00 for RAC Blueprints). Non-US add $15.00 per book or CD-ROM for air mail ($30.00 for NPRD or VZAP, $50.00 for EPRD, $4.00 for RAC Blueprints).				
Total				

Name _____

Company _____

Division _____

Address _____

City _____ **State** _____ **Zip** _____

Country _____ **Phone** _____ **Ext** _____

Fax _____ **E-mail** _____

Method of Payment:

Company/Personal Check Enclosed (Make checks payable to IITRI/RAC)

Credit Card #: _____ **Exp Date:** _____

Type (circle): American Express VISA Mastercard

A minimum of $25.00 is required for credit card orders

Name on Card _____

Signature _____

Billing Address _____

Company/Government Purchase Order   **Send Product Catalog**

*Visit <http://rac.iitri.org/cgi-rac/iPC/> for a complete list of RAC products.

pRISM

System Reliability Assessment Software

RACRates Next Generation
Component Failure Rate Models
System-Level Process Assessment
Operating & Non-Operating Reliability
Historical Data on Similar Systems

The New Methodology

everything else is History

Reliability Analysis Center

Free Demo: http://rac.iitri.org

IIT Research Institute/
Reliability Analysis Center
201 Mill Street
Rome, NY 13440-6916

The Journal of the

RAC

Reliability Analysis Center

(315) 337-0900	**General Information**
(888) RAC-USER	**General Information**
(315) 337-9932	**Facsimile**
(315) 337-9933	**Technical Inquiries**

rac@iitri.org   **via e-mail**

http://rac.iitri.org   **Visit RAC on the Web**